

ELECTRONIC SECURITY COMPONENT

Field of the Invention

The present invention relates to electronic devices, and, more particularly, to an electronic security component in which sensitive information is
5 processed.

Background of the Invention

Electronic security components processing sensitive information are used especially in smart cards. Applications of these cards include accessing
10 banks for banking applications, and for remote payments for television, gasoline distribution and highway tolls, for example. These electronic security components have to process confidential data that must be shielded against any attempt at espionage for
15 fraudulent purposes. The confidential data travels through the data bus of the component between a central processing unit (processor) and peripherals, such as memories.

Different methods can be implemented to
20 discover these confidential data elements. In particular, one physical characteristic that can be observed external the electronic component is its current signature which depends on the passage of data in transit on the data bus. The data bus has a high

capacity because it circulates throughout the component.

For this reason, the output interface includes three-state selection switches sized to let
5 through high current for charging or discharging the line capacitor. Since the data bus is an 8-bit data bus, it includes eight large selector switches that are activated to apply a data element to this bus. Consequently, there is high current consumption during
10 the selection switching of the switches.

Summary of the Invention

In view of the foregoing background, it is an object of the present invention to prevent the identification of data elements traveling through the
15 bus or at least make this identification difficult.

It is another object of the present invention to use data encryption to improve the protection of confidential data.

Yet another object of the present invention
20 is to implement data encryption at low cost whether in terms of silicon surface area, connection lines between the peripherals and the central processing unit, or data-processing time.

Another object of the present invention is to
25 implement a data encryption system that can be adapted to all classes of components in a relatively straight forward manner without extra cost of customized design.

In view of these and other objects, advantages and features, one approach is to provide a
30 component whose central processing unit and peripherals, which have to process sensitive data received or transmitted on the data bus, each comprise an encryption/decryption cell. Each encryption/decryption cell applies the same secret key
35 produced locally by each cell at each clock cycle to a

data element received or to be transmitted in the clock cycle.

Using the convention according to a clock cycle starting at the high level, the writing of a data element of the bus is done at the low level and the reading of a data element on the bus is done on the leading edge. Thus, in a given clock cycle, a data element may be encrypted with a secret key produced by the cell of a sender and transmitted on the bus during the write period on the bus. This encrypted data element may be read by an addressee and decrypted in the cell of this addressee with the secret key locally produced by this cell.

The two locally produced secret keys have the particular feature of being identical. Thus, according to the invention, the secret key is produced locally in each cell from a synchronous random signal applied to all. This is done in one clock cycle for the encryption of a data element given by a sender, and for the decryption of this data element encrypted by an addressee.

The present invention therefore relates to an electronic component comprising a two-way bus through which data elements travel in transit between peripherals and a central processing unit at the rate of a clock signal. The central processing unit and at least one of the peripherals each comprises a data encryption/decryption cell using the same secret key. A current value of the secret key is produced locally in each cell at each clock cycle from a random signal synchronous with the clock signal, and is applied to each of the cells by a one-way transmission line.

Brief Description of the Drawings

Other features and advantages of the invention shall be described in detail in the following

description by way of a non-restricted indication and with reference to the appended figures, of which:

Figure 1 shows an exemplary architecture of an electronic component to which the present invention
5 can be applied;

Figure 2 shows a simplified architecture of an electronic component according to the present invention;

Figure 3 is an exemplary timing diagram of
10 the data and control signals of the electronic component shown in Figure 2;

Figure 4 is a block diagram of an encryption/decryption cell according to the present invention;

Figure 5 shows the encryption/decryption cell comprising a conditional circuit applicable to the central processing unit according to the present
15 invention;

Figure 6 is a detailed drawing of the encryption and decryption circuits in the cell
20 according to the present invention; and

Figure 7 is a block diagram of a synchronous random signal generator that can be used in the present invention.

25 **Detailed Description of the Preferred Embodiments**

Figure 1 shows an exemplary architecture of an electronic security component to which the present invention can be applied. In this example, the electronic component is more particularly designed for
30 smart card type applications. Its external connections are thus limited to two series-connected input/output pads, a clock pad CALK to receive an external clock signal, a pad to receive a resetting signal RST, and the logic supply pads Vcc and Gnd.

35 The architecture of this component comprises a central processing unit CPU and peripherals P1, P2,

P3 which, in the example, are respectively a non-volatile memory (e.g., an EEPROM type), a RAM type working memory, and a ROM type program memory. An interface circuit INT provides the interface between
5 the serial input/output pads and the parallel bus of the component which is subdivided into an address bus AD-BUS, and a data bus DATA-BUS to which the central processing unit and the peripherals are connected.

In this architecture, it is also planned to
10 have a circuit CAP for access control to the peripheral which receives the most significant bits A7-A5 from the address bus AD-BUS. It contains a space allocation table for the physical addressable space of the component and gives especially the selection signals
15 P1-sel, P2-sel and P3-sel of the peripherals P1, P2, P3 as a function of the decoded address. In this example, the peripherals receive only the least significant bits A5-A0 from the address bus.

Depending on the instructions that the
20 central processing unit receives externally, it gives control signals CTL, especially a read/write signal RW, to be applied to the peripherals. Finally, the pad CALK gives the clock signal PHI applied to all the circuits of the component. That is, the clock signal
25 PHI is applied to the central processing unit, the peripherals, the interface circuit, and the peripheral access control circuit in the example.

In the invention, it is sought to secure this circuit by preventing the determining of the data
30 elements that travel through the internal data bus DATA-BUS through observation of the current consumption of the component. Thus, as shown in Figure 2 in a simplified representation of the architecture of the component of Figure 1, an encryption/decryption cell is
35 placed in the central processing unit and in each of the peripherals that read or write sensitive data on the data bus, i.e., in the peripherals P1 and P2.

These cells are referenced Kcell_{CPU}, Kcell_{p1} and Kcell_{p2} in Figure 2.

The electronic component according to the invention then comprises a random signal generator
5 KEY_GEN synchronized with a clock signal on a one-way transmission line to apply this signal to each of the encryption/decryption cells planned in the component. Each of these cells is furthermore connected to the input/output of the data bus DATA-BUS.

10 Figure 3 shows a timing diagram corresponding to a read operation in which the central processing unit reads a data element of the peripheral P1 followed by a write operation in which the central processing unit writes the data element in the peripheral P1. This
15 timing diagram illustrates the principle of the invention.

This timing diagram shows two clock cycles referenced cycle 1 and cycle 2, the synchronous random signal K_{IN}, the secret key KEY computed locally in each
20 cell, the address bus AD-BUS, the selection signal P1-sel of the peripheral P1, the read/write control signal RW whose low level corresponds to a write command and whose high level corresponds to a read command (by convention), and the data bus DATA-BUS. Considering
25 the first clock cycle shown (cycle 1), it has a corresponding value KEY₀ of the secret key that is computed locally in each cell from the new input value of the random signal K_{IN}, which is 0 in the example.

The peripheral P1 is selected (P1-sel at the
30 high level) in read mode (RW at the high level) at the address applied to the address bus AD-BUS. The cell Kcell_{p1} of peripheral P1 gives on the bus the data element read at this address, which is encrypted with the current value of the secret key KEY₀ that is
35 locally computed by this cell Kcell_{p1}. This data element is transmitted on the bus on the low level of the cycle 1 of the clock signal. The encrypted data

element is stored in an input register of the central processing unit CPU on the leading edge of the cycle 1 of the clock signal, and decrypted by the cell Kcell_{CPU} with the current value KEY₀ of the secret key locally
5 computed by this cell Kcell_{CPU}.

Considering the second clock cycle shown (cycle 2), it has a corresponding value KEY₁ of the secret key locally computed in each cell from the new input value of the random key K_{IN}, which is 1 in the
10 example. The peripheral P1 is selected (P1-sel at the high level) in write mode (RW at the low level) at the address applied to the address bus AD-BUS. The cell Kcell_{CPU} of the central processing unit gives on the bus the data element to be written at this address, which
15 is encrypted with the current value of secret key KEY₁ that is locally computed by this cell Kcell_{CPU}. This data element is transmitted on the bus on the low level of the cycle 2 of the clock signal. The encrypted data element is stored in an input register of the
20 peripheral P1 on the leading edge of the cycle 2 of the clock signal, and decrypted by the cell Kcell_{P1} with the current value KEY₁ of the secret key locally computed by this cell Kcell_{P1}.

A general block diagram of an encryption/
25 decryption cell Kcell according to the invention is shown in Figure 4. This cell is such that it locally computes the current value of the secret key used both for encryption and for decryption. The cell Kcell has a register KEYREG that gives the secret key KEY for the
30 encryption and decryption. It is an n-stage shift register sequenced by the clock signal PHI and receives the random data signal K_{IN} at input synchronous with the clock signal PHI. The register KEYREG gives the current value of the secret key KEY at output for the current
35 clock cycle, whose value is a polynomial function of the n most recent values of the random signal K_{IN}. The

secret key thus takes a new random value at each clock cycle.

The register is preferably a feedback shift register. That is to say, it has combinational logic gates to apply the output bit of certain stages to the input of other stages of the register. This makes it possible to obtain valuable polynomial functions. Preferably, an irreducible polynomial function is implemented to improve the resistance of the encryption.

The cell Kcell has an encryption module A and a decryption module B to which the secret key KEY given by the register KEYREG of the cell is applied. In the example, the mathematical function implemented in the encryption module is the XOR function which has the particular feature of being also the function to be applied in the decryption module and of being easy to implement.

The encryption module A receives inter alia an internal data element Dout from the circuit in which the cell Kcell is placed and the secret key KEY produced locally by the register KEYREG. At output, it delivers an encrypted data element applied to the data bus DATA-BUS through the output interface of the circuit, which is symbolically shown in the figure by a controlled inverter.

The decryption module B receives a data element from the data bus and the secret key KEY locally produced by the register KEYREG. At output, it gives a decrypted data element Din. In one improvement shown in Figure 5, the encryption/decryption cell of the central processing unit comprises, in addition to the elements described here above, a conditional circuit used for the application to the encryption and decryption modules of either the secret key KEY or a neutral key KN corresponding to the neutral value for

the encryption operation considered. In the exemplary XOR operation, this neutral value is the zero value.

This improvement is used to avoid implementing an encryption/decryption cell in all the circuits connected to the data bus in the component considered, and is implemented in only those cells that handle data elements to be protected. It is therefore planned that the control circuit PAC for access to the peripherals (shown in Figures 1 and 2) will give an encryption enabling signal SCRAMBLE to the central processing unit CPU whenever it decodes the address of a peripheral of this kind. In practice, this access control circuit finds this information in its physical address allocation table.

It will be noted that the information SCRAMBLE in the example given by the access control circuit is placed outside or external the central processing unit in the exemplary architecture shown in Figures 1 and 2. This is not absolutely restrictive. The information SCRAMBLE is more generally given by an address decoding circuit of the component.

The conditional circuit of the cell Kcell_{CPU} according to the improvement of the invention comprises a multiplexer MUX receiving the secret key KEY and the neutral key KN at input. At output, this conditional circuit gives the key selected by the encryption enabling signal SCRAMBLE, which is applied to the encryption and decryption modules of this cell Kcell_{CPU}.

Figure 6 gives a slightly more detailed view of an encryption/decryption cell according to the present invention. If we consider an 8-bit data bus, the secret key must include at least as many bits. The register KEYREG has eight stages to give eight secret key bits referenced K0 to K7. Each of these eight data bits is applied in the encryption module A, and in the decryption module B to a corresponding XOR gate

receiving the same-order data bit to be encrypted or decrypted at input. Each of these modules thus comprises eight XOR gates, one per bit.

This figure shows an exemplary embodiment of
5 a shift type feedback register KEYREG. The references E0 to E7 designate the eight stages of the register, respectively giving the bits K7 to K0 of the secret key. These stages may be D-type flip-flop circuits, for example.

10 In the exemplary embodiment shown, the stage E0 receives at input the random signal KIN combined in an XOR gate with the bit K0 given by the last stage E7 of the register, and at output it delivers the bit K7. The stage E1 receives at input the bit K7 combined in
15 an XOR gate with the bit K0. At output it delivers the bit K6. The stages E2, E3 and E4 receive at input the bits given by the preceding stage, and deliver at output the bits K5, K4 and K3 respectively. The stage E5 receives the bit K3 at input which is combined in an
20 XOR gate with the bit K0, and delivers the bit K2 at output. This stage E6 receives the bit K2 at input which is combined in an XOR gate with the bit K0, and delivers the bit K1 at output. The stage E7 receives the bit K1 at input and delivers the bit K0 at output.

25 Figure 7 represents an exemplary generator KEYGEN of the random signal KIN. In this example, the generator comprises a pseudo-random generator to give a random clock signal that is applied to the D input of a flip-flop circuit BS to be synchronized by the clock
30 signal PHI. This flip-flop circuit therefore receives the clock signal PHI at its clock input, and gives at its Q output a random signal KIN that is synchronized with the clock signal PHI.

It is very difficult in principle to
35 determine the value taken by the random signal by observing the power consumption of the component arising from the switching operations on the

transmission line of the synchronous random signal KIN because the capacitance of this one-way line is very low. However, in one improvement of the invention, it is planned that the generator of the synchronous random
5 signal will comprise a circuit CMC for masking the consumption due to the selection switching operations on this transmission line. In the example, this circuit CMC is connected between the output of the synchronization flip-flop circuit BS and the
10 transmission line.

There are different consumption masking circuits of varying degrees of efficiency. An exemplary non-exhaustive embodiment is shown in Figure 7. It has two D-type flip-flop circuits, B1 and
15 B2. The first flip-flop circuit B1 receives the Q output of the synchronization flip-flop circuit BS as a data input, and the clock signal from the bus PHI as a clock input. The Q output is connected by an interface element (driver) I1 to the transmission line.

20 The complementary /Q output of the flip-flop circuit B1 is applied to a combinational circuit whose output S is applied to the data input of the second flip-flop circuit B2. The Q output of this second flip-flop circuit B2 is connected to a capacitor CKN
25 whose capacitance corresponds to the parasitic capacitance CK of the transmission line perceived by the output interface I1 of the generator KEYGEN.

The combinational circuit, in the example, has a first OR gate receiving the Q outputs of the
30 synchronization flip-flop circuit and of the second flip-flop circuit B2 as inputs. A second OR gate receives the output of the first gate and the complementary output /Q of the first flip-flop circuit B1 as inputs. With a combinational circuit of this
35 kind, complementary transitions are obtained in the flip-flop circuits B1 and B2 so that the same

consumption due to the transmission of the signal KIN is observed at each clock cycle.

In a another improvement of the invention, it is planned that the random signal KIN will be
5 transmitted on the transmission line only after activation by the central processing unit of an encryption activation signal ENENCRYPT. This can be done simply by forcing the resetting of the flip-flop circuits.

10 Figure 7 thus shows an AND type logic gate receiving, as inputs, the resetting signal RST of the component which is active at zero, and the enabling signal EN-ENCRYPT. This signal is at zero by default. Thus, so long as the enabling signal is at zero after
15 the setting, the flip-flop circuits B1 and B2 are set at zero, and the transmission line is set at zero. As soon as it is set at 1 by the central processing unit, the random signal is sent.

It will be noted that the two improvements of
20 the generator of the synchronous random signal, namely the masking of consumption and the enabling of encryption, can be implemented independently of each other. Thus, in certain components, it is possible to implement only one of these improvements. To this end,
25 it will be noted that the improvement relating to encryption enabling can be implemented independently of the masking circuit. For example, this may be done using an AND logic gate receiving the synchronous random signal KIN and the activation signal EN-ENCRYPT as
30 inputs, and connected at output to the transmission line.

The use of encryption/decryption cells according to the invention thus gives efficient protection for sensitive data. This protection costs
35 little in terms of design, implementation and processing time for the component. In particular, the design is facilitated by the user of encryption/

decryption cells that are identical in all the peripherals.

The encryption/decryption cell of the central processing unit comprises an encryption-enabling option
5 by which it is possible not to implant a cell necessarily in all the peripherals. The random signal generator has two embodiment options, which are a consumption masking option and an encryption/decryption activation option.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216